## Remarks

The following remarks are responsive to the Final Office Action of October 11, 2007.

At the time of the Office Action, claims 1-54 were pending. As indicated above, independent claims 1, 18, 26, 37 and 44 are being amended to include the limitations of dependent claims 16, 25, 29, 42 and 47, respectively, and claims 16, 25, 29, 42 and 47 are being canceled. Also, the dependencies of claims 17 and 43 are being changed as appropriate to depend from their respective amended independent claims instead of the canceled claims. Hence, the above amendments should be entered since no new material is being added to the claims. Upon entry of the amendments, claims 1-15, 17-24, 26-28, 30-41, 43-46 and 48-54 will remain pending.

Claims 1-54 stand rejected under 35 U.S.C. § 103(a) as being obvious over U.S. Patent No. 6,971,017 to Stringer et al. (hereinafter Stringer) in view of U.S. Patent Application Publication No. 2001/0018739 to Anderson et al. (hereinafter Anderson). This rejection is respectfully traversed.

Regarding amended independent claim 1, claim 1 recites a method, device, delegation server, computer program product of electronically signing documents, comprising the steps of generating a token of delegation from a first signatory to a second signatory, and associating the delegation token with a document signed electronically by means of a cryptographic key of the second signatory. The delegation token contains delegation data electronically signed for the first signatory, and the delegation data include an identifier of the second signatory. Further, the delegation token is generated by a server in response to a request sent by the second signatory in connection with the signing of the document, where said request is accompanied by data depending on the document to be signed which are included in said delegation data to generate the delegation token.

The Examiner contends that Stringer discloses these features but admits, with regard to independent claims 18, 26, 37, and 44, that "Stringer does not specifically disclose a document signed electronically by means of a cryptographic key. However, the Examiner contends that

Anderson discloses wherein a document signed electronically by means of a cryptographic key" (see Office Action, page 5, line 19 - page 6, line 12; page 13, lines 2 - 6, lines 11-13; page 14, line I - page 15, line 7; page 15, lines 13 - 16).

This rejection will first be addressed with regard to independent claims 1, 18, 26, 37 and 44 of the present application.

Applicants submit that the claims are directed to electronically signing documents associated with a delegation token, while the documents stored in Stringer's server 102 are not signed. Further, Applicants respectfully submit that Stringer relates to a method of accessing documents or services stored on a document server 102 to which certain users (e.g., User A) have access rights while other users (e.g., User B) do not have registered access rights.

In other words, as shown in Fig. 2 and described in column 6, line 7 - column 7, line 37 of Stringer, the method in Stringer can be described simply as performing the following operations:

User A with registered access rights establishes secure session with the document server;

Document server authenticates user A as a registered user of the document server;

User A sends a request for the directory listing of files or service to the document server;

Document server transmits directory listing to User A;

User A invokes a script for creating a URL token for the selected document or service from the directory listing;

Document server creates a new entry in the token database with a unique token ID and the path of the selected document(s) or service (s);

Document *server* transmits the unique token ID associated the token in the token database recording the selected path to User A;

User A must receive digital certificate information from User B who does not have registered access rights before the URL token is signed by User A's private key;

User A transmits URL token signature to document server which record URL token signature in the token database;

User A transmits URL token to User B; and

Then User B is free to redeem the URL token at the document server.

During the entire process as described in Stringer, the documents stored in the document server 102 are not signed by any user such as User A or B. The Examiner states that "the Stringer prior art also discloses signing a document," citing col. 10, lines 42 – 49 of Stringer. (See page 2, line 16 - page 3, line 5 of the Office Action). However, regarding this passage, in fact, Stringer's User A would like to "provide user B along with the URL token and to the document server alone with signature of the URL token a signed or unsigned cryptographic digest of the content or part of the content of the selected document or service which may be included with access rights information specified in the signature content 302." (See Stringer, col. 10, lines 23 - 52). In other words, User A might sign the digest of the content or part of the content of the selected document *but not the selected document itself,* as recited in the independent claims of the present application. Accordingly, the documents stored in Stringer's server 102 are not signed, while the claims of the present application recite features for electronically signing documents associated with a delegation token.

In addition, in the claimed embodiments, the documents are signed electronically by means of a cryptographic key of the second signatory, which would be "User B" in Stringer according to the Examiner's characterization. However, in Stringer's method, User B does not sign anything. Through the process described above, User B merely receives the URL token from the User A and then redeems the URL token at the document server in order to access the document or service on the document server without signing anything.

Furthermore, the independent claims of the present application recite feature relating to associating a delegation token with a signed document, whereas Stringer associates the "URL token" with a path to an unsigned document during the process in Stringer, as mentioned above. The independent claims of the present application also recites generating the delegation token by a server, whereas Stringer's URL token is not generated by the document server 102, but by User A's device 106. In particular, during the Stringer process mentioned above, "upon receiving the transmitted directory listing (i.e., a set of paths to documents or services to which user A has access) at 206, user A invokes a script for creating a URL token for the selected document or service from the directory listing and then sends it to document server. After receiving the selected paths, the server creates a new entry in the token database with a unique token ID and the path of the selected documents or services and then sends the token ID to User A. User A signs the content of token ID 314, user B's public key 312, a document (or service) path 316 and token rights 318 with User A's private key and then sends the URL token signature to document server which records the URL token signature in the token database" (See FIG. 2; column 6, line 7-column 7, line 37).

Although Stringer may state that "the script invoked for creating a URL token may be stored on the script server 122," it can be considered that the URL token is issued and generated by User A, and the token database in is used to store the URL token. Accordingly, the document server 102 records the URL token in the token database instead of generating the URL token (see also, column 6, line 35-39 of Stringer).

On the other hand, at least independent claim of the present application recites generating the delegation token in response to a request sent by the second signatory, which would be equivalent to User B in Stringer according to the Office Action. However, Stringer's URL token is generated in response to an invocation by User A at 208.

Based on Springer's process, the URL token is generated in response to the script invoked by User A (See column 6, line 35-39 of Stringer). Until this time, User B, which can be considered as a second signatory, sends User B's certificate information and not the request to User A nor the document server. In other words, until the URL token is generated, User B does not even communicate with the document server, whereas the independent claims of the present application recite features relating to generating the delegation token by a server in response to a request sent by the second signatory.

In addition, Stringer does not disclose that the request is accompanied by data depending on the document to be signed, with the data being included in the delegation data to generate the delegation token as in the claimed embodiments. As described on page 13, lines 6-11 of the specification, the embodiments of the present invention can thus generate a token depending on the document or message to be signed and therefore to avoid undesirable replays of the token. Applicants respectfully submit that Stinger fails to teach or suggest this feature.

Furthermore, the Examiner states that "Anderson discloses wherein a document signed electronically by means of a cryptographic key" (See page 6, lines 8-12 of the Office Action,). However, Applicants respectfully submit that the claimed aspects of the present invention do not relate broadly to signing of documents, but rather to signing documents securely by delegates, which is suggested neither by Stringer nor Anderson. Therefore, Applicants respectfully submit that one skilled in the art would not have found it obvious or possible to combine the teachings of Stringer and Anderson to have achieved the embodiments of the present invention even as recited in amended independent claims 1, 18, 26, 37 and 44.

Concerning claims 2, 19, and 38, the Examiner states "that Stringer discloses a method, device, computer program product according to claims 1, 18, 37, wherein the electronic signature performed by means of the cryptographic key of the second signatory is applied to the document accompanied by the delegation token." Moreover, the Examiner mentions that "Stringer does not specifically disclose whereby the electronic signature performed by means of the cryptographic key of the second signatory is applied to the document," but Anderson discloses the messing features (See page 7, line 2 of the Office Action).

Applicants respectfully submit that the "URL token" in Stringer is associated with a path to an unsigned document (see FIG. 2; column 6, line 7 - column 7, line 37 of Stringer). On the contrary, the claims of the present application recite features relating to achieving the electronic signature by applying the cryptographic key of the second signatory to the document accompanied by the delegation token. Also, Applicants respectfully submit that Anderson merely teaches a document signed electronically by means of a cryptographic key. Therefore, Stringer and Anderson do not suggest the features recited in claims 2, 19, and 38 of the present application.

Concerning claims 3, 20, and 39 of the present application, the Examiner states that "Stringer discloses a method, device, and computer program product according to claims 1, 18, 37, wherein the electronic signature performed by means of the cryptographic key of the second signatory is applied on the other hand to authenticated attributes including the delegation token." Furthermore, the Examiner states that "Stringer does not specifically disclose whereby the electronic signature performed by means of the cryptographic key of the second signatory is applied on the one hand to the document," but Anderson discloses this (see page 7 of the Office Action).

Again, as discussed above, Applicants respectfully submit that Stringer's signature content includes: User B's public key, token Id, document path and token rights without authenticated attributes, whereas our application discloses that the electronic signature performed by means of the cryptographic key of the second signatory is applied on the other hand to authenticated attributes including the delegation token (see Fig 2, item 218 and column 6, line 55-column 7, line 24 of Stringer). In addition, Applicants submit that Anderson discloses a document signed electronically by means of a cryptographic key. Therefore, Stringer and Anderson do not teach or suggest the features recited in dependent claims 3, 20, and 39.

Referring to claims 4 and 40, the Examiner states that "Stringer discloses a method, device, and computer program product according to claims 1, 37, wherein the delegation token is associated with the document of the second signatory without itself being signed by means of the cryptographic key of the second signatory." In addition, the Examiner states that "Stringer does not specifically disclose whereby the document signed by means of the cryptographic key," but contends that this feature is taught by Anderson. (see page 8 of the Office Action).

Based on the foregoing arguments, Stringer associates the "URL token" with a path to an unsigned document during the process in Stringer (see FIG. 2 and column 6, line 7 - column 7, line 37 of Stringer), whereas the embodiments of the present invention achieve the electronic signature performed by applying the cryptographic key of the second signatory to the document accompanied by the delegation token. Moreover, the URL token in Stringer is signed by User A's private key to obtain the URL token signature (See FIG. 2, item 218 and column 6, line 55 - column 7, line 24 of Stringer), whereas the delegation token, as recited in the claims of the present application, is associated with the signed document without itself being signed by the cryptographic key of the second signatory. In addition, Anderson simply discloses a document signed electronically by means of a cryptographic key. Therefore, the teachings of Stringer and Anderson would not have rendered the features of the claims 4 and 40 obvious.

Referring to claims 5, 21, 32, and 50, the Examiner states that "Stringer discloses a method, device, delegation server, computer program product according to claims 1, 18, 26, 44, wherein the delegation data further include data describing a validity period of the delegation token." (see page 9 of the Office Action).

Applicants submit, however, that in Stringer, "the audit information associated with the token includes: when the token was issued, the duration the token is valid, and whether the token is valid, and how the token was used, how many times it was accessed" (see column 4, lines 53-67 of Stringer). However, as discussed above, Applicant's delegation mechanism is quite distinct from the mechanism described by Stringer. Also, Anderson fails to make up for the deficiencies in Stringer. Thus, Applicants submit that claims 5, 21, 32, and 50 should be allowable.

With regard to claims 6, 22, 33, and 51, the Examiner states that "Stringer discloses a method, device, delegation server, computer program product according to claims 1, 18, 26, 44, wherein the delegation data further include description data of delegated powers conferred by the token" (see page 9 of the Office Action). Applicants respectfully submit that in Stringer, "the access rights associated with the token specify information such as: how the token may be used, the version of the document or service to which access may be given, and whether the token is delegable" (see column 4, line 53 - column 5, line 3 of Stringer). However, as discussed above, Applicant's delegation mechanism is quite distinct from the mechanism described by Stringer, and Anderson fails to make up for the deficiencies in the teachings of Stringer. Thus, Applicants submit that these claims should be allowable over Stringer and Anderson.

Referring to claims 7, 24, 34, and 52, the Examiner states that "Stringer discloses a method, device, delegation server, computer program product according to claims 1, 18, 26, 44, wherein the delegation token further comprises timestamp information for the token." (See page 9 of the Office Action). Applicants respectfully submit that in Stringer, "the audit information associated with the token includes: when the token was issued, the duration the token is valid, and whether the token is valid, and how the token was used, how many times it was accessed" (see column 4, lines 53-67 of Stringer). However, as discussed above, Applicant's delegation mechanism is quite distinct from the mechanism described by Stringer. Also, Anderson fails to make up for the deficiencies in the teachings of Stringer. Thus, Applicants submit that the feature of the timestamp information for the delegation token as recited in claims 7, 24, 34, and 52 should be patentable over Stringer and Anderson.

With regard to claims 8, 9, 23, and 53, Examiner states that "Stringer discloses a method, device, delegation server, computer program product according to claims 1, 18, 18, 44, wherein a revocation server is provided for storing information on possible revocation of the delegation token by the first signatory" (see page 10 of the Office Action). Also, with regard to claim 9 in particular, claim 9, the Examiner states that "Stringer discloses a method, according to claim 8, wherein the delegation data further include an access address to the revocation server." However, Applicants respectfully submit that Stringer merely mentions that in one embodiment, "user A is provided mechanisms for audit and revocation (or modification) of access to issued URL tokens" and "browsing the token database also permits user A to revoke issued URL tokens or refresh expiry information of issued URL tokens" (see column 10, lines 57-67 of Stringer), without mentioning using a special revocation server as recited in these claims of the present application. In the claimed embodiments, a revocation server is provided for storing information on possible revocation of the delegation token by the first signatory. Accordingly, Stringer does not teach or suggest the features of claims 8, 9, 23, and 53. Anderson also fails to make up for the deficiencies in the teachings of Stringer. Hence, these claims should be allowable.

Referring to claim 10, the Examiner states that "Stringer discloses a method, according to claim 1, wherein the delegation data are signed electronically by means of a cryptographic key of the first signatory" (See page 10 of the Office Action). Applicants submit that the URL token in Stringer is considered as the delegation token including the delegation data being signed electronically by means of a cryptographic key of the User A being considered as the first signatory in our application (see FIG. 3 and column 6, line 55 - column 7, line 24 of Stringer). However, according to the arguments already detailed above, Applicant's delegation mechanism is quite distinct from the mechanism described by Stringer. Also, Anderson fails to make up for the deficiencies in the teachings of Stringer. Hence, Applicants submit that claim 10 should be allowable over Stringer and Anderson

With regard to claims 11, 36, and 54, the Examiner states that "Stringer discloses a method, device, delegation server, computer program product according to claims 1, 26, 44, wherein the delegation data further include an identifier of the first signatory and are signed electronically by means of a cryptographic key of a third party" (see page 10 of the Office Action). However, Applicants respectfully submit that Stringer fails to teach or suggest that the delegation further includes an identifier of the first signatory and are signed electronically by means of a cryptographic key of a third party as these claims state. Anderson also fails to make up for the deficiencies in these teachings. Hence, these claims should be allowable.

Referring to claims 12 and 27, the Examiner states that "Stringer discloses a method, server according to claims 1, 26, wherein the delegation token is associated by the second signatory with the document of the second signatory." Furthermore, the Examiner admits that "Stringer does not specifically disclose whereby the document signed electronically by means of a cryptographic key," but contends that Anderson discloses this feature. (See page 11 of the Office Action). As discussed above, Applicants respectfully submit that Stringer, either alone or in combination with Anderson, does not disclose that the delegation token is associated by the second signatory with the document of the second signatory.

With regard to claim 13, the Examiner states that "Stringer discloses a method, according to claim 1, wherein the delegation token is sent to the second signatory by the server" (See page 11 of the Office Action). However, according to the arguments already detailed above, the URL token considered as delegation token in our application is sent to User B considered as the second signatory by User A but not the server (Fig. 2 and column 6, line 7 through column 7, line 37 of Stringer). Thus, Stringer does not disclose that the delegation token is sent to the second signatory by the server as claim 13 states. Anderson also fails to make up for this deficiency.

Referring to claims 14, 28, 41, and 46, the Examiner states that "Stringer discloses a method, server, computer program product according to claims 13, 27, 37, 45, wherein the delegation token is associated with the signed document by an applet downloaded from the server to a station of the secondary signatory." (See page 12 of the Office Action). As discussed above, Applicants submit that Stringer does not disclose a method, a server, or a computer program product as recited in claims 13, 27, 37, and 45 where the delegation token is associated with the signed document by an applet downloaded from the server to a station of the secondary signatory. Anderson also fails to make up for the deficiencies in the teachings of Stringer.

Concerning claims 15, 31, and 49, the Examiner states that "Stringer discloses a method, server, computer program product according to claims 1, 26, 44, wherein the second signatory submits the signed document to the server, and wherein the server associates the signed document with the delegation token." In addition, the Examiner admits that "Stringer does not specifically disclose whereby the second signatory signs the document electronically," but contends that Anderson discloses this feature. (See page 12 of Office Action).

Applicants submit that as discussed above, the User B, which can be assumed to be a second signatory, does not submit anything to the server except the request for accessing documents or service on the server with the URL token (see FIG. 4 and column 6, line 7 - column 7, line 37 of Stringer), whereas the second signatory in the claimed embodiments submits the signed document to the server and the server associates the signed document with the delegation token. Therefore, Stringer, either alone or in combination with Anderson, does not disclose, teach or suggest the features of claims 15, 31, 49.

Referring to claims 17, 30, 43, and 48, the Examiner states that "Stringer discloses a method, server, computer program product according to claims 16, 26, 42, 44, wherein said data depending on the document to be signed comprise a code obtained by hashing the document" (see page 13 of Office Action). Applicants submit that the signature content including User B's public key, token ID, document path and token rights, and not the data depending on the document to be signed, is processed by a hash function in the URL token signature generator (see FIG. 3 and column 6, line 55 - column 7, line 3 of Stringer). Therefore, Stringer does not disclose that the data depending on the document to be signed comprises a code obtained by hashing the document. Anderson also fails to make up for this deficiency.

Concerning claim 35, the Examiner states that "Stringer discloses a server according to claim 26, wherein the delegation data further include an access address to a revocation server provided for storing information on possible revocation of the delegation token by the first signatory" (see page 13 of the Office Action). However, as discussed above, Stringer does not disclose a server as recited in claim 26 where the delegation data further includes an access address to a revocation server provided for storing information on possible revocation of the delegation token by the first signatory. Anderson also fails to make up for this deficiency.

With regard to claim 45, the Examiner states that "Stringer discloses a computer program product according to claim 44, further instructions means for sending the delegation token to the second signatory for association with the document signed electronically by means of the cryptographic key of the second signatory" (see page 15 of the Office Action). However, as discussed above, Applicants submit that, Stringer does not disclose a computer program product as recited in claim 44. Anderson also fails to make up for these deficiencies.

For at least the above reasons, Applicants respectfully submit that all claims should be allowable.

The application is considered in good and proper form for allowance, and the Examiner is respectfully requested to pass this application to issue. If, in the opinion of the Examiner, a telephone conference would expedite the prosecution of the subject application, the Examiner is invited to call the undersigned attorney.

Respectfully submitted,

/brian c. rupp/

Brian C. Rupp, Reg. No. 35,665
One of Attorneys for Applicant(s)
DRINKER BIDDLE & REATH LLP
191 N. Wacker Drive, Suite 3700
Chicago, Illinois 60606-1698
(312) 569-1000 (telephone)
(312) 569-3000 (facsimile)
Customer No.: 08968

Date: January 11, 2008